



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,511	04/01/2004	Huw Edward Oliver	300203615-4	1299

7590 07/26/2007
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

CHERY, DADY

ART UNIT	PAPER NUMBER
----------	--------------

2616

MAIL DATE	DELIVERY MODE
-----------	---------------

07/26/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/815,511

Applicant(s)

OLIVER ET AL.

Examiner

Dady Chery

Art Unit

2616

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 April 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 04/01/2004.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 16 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. "a data storage media comprising program " is not being executed by a computer. This subject matter is not limited to that which falls within a statutory category of invention because it is not limited to a process, machine, manufacture, or a composition of matter. Data storage does not fall within a statutory category since it is clearly not a series of steps or acts to constitute a process, not a mechanical device or combination of mechanical devices to constitute a machine, not a tangible physical article or object which is some form of matter to be a product and constitute a manufacture, and not a composition of two or more substances to constitute a composition of matter.

Double Patenting

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims

Art Unit: 2616

are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1 -16 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim1 of copending Application No. 10/815512.

Claims 1 -16	
Present application	Copending application
<p>1. A method for controlling a computer entity to participate in a peer to peer network of a plurality of computer entities, said method comprising: for each computer entity: operating a peer to peer protocol for enabling said computer entity to utilise resources of at least one other said computer entity of said network, and for enabling at least one other said computer entity of said network to utilise resources of said computer entity; and operating a process for managing at least one other said computer entity in said network, whenever said resources are not being used by at least one service application at a higher level layer than said peer to peer protocol.</p>	<p>1. A method for controlling a computer entity to participate in a peer to peer network of a plurality of computer entities, said method comprising: for each computer entity: operating a peer to peer protocol for enabling said computer entity to utilise resources of at least one other said computer entity of said network, and for enabling at least one other said computer entity of said network to utilise resources of said computer entity; and operating a process for managing at least one other said computer entity in said network, whenever said resources are not being used by at least one service application at a higher level layer than said peer to peer protocol. .</p>

Present application	Copen ding application
<p>1. A method for controlling a computer entity to participate in a peer to peer network of a plurality of computer entities, said method comprising: for each computer entity: operating a peer to peer protocol for enabling said computer entity to utilise resources of at least one other said computer entity of said network, and for enabling at least one other said computer entity of said network to utilise resources of said computer entity; and operating a process for managing at least one other said computer entity in said network, whenever said resources are not being used by at least one service application at a higher level layer than said peer to peer protocol.</p> <p>2.The method as claimed in claim 1, wherein said process of managing at least one other computer entity in said network</p>	<p>1. A method for controlling a computer entity to participate in a peer to peer network of a plurality of computer entities, said method comprising: for each computer entity: operating a peer to peer protocol for enabling said computer entity to utilise resources of at least one other said computer entity of said network, and for enabling at least one other said computer entity of said network to utilise resources of said computer entity; and operating a process for managing at least one other said computer entity in said network, whenever said resources are not being used by at least one service application at a higher level layer than said peer to peer protocol. .</p> <p>2.The method as claimed in claim 1, wherein said process of managing at least one other computer entity in said network</p>

comprises: determining at least one policy by which said computer entity will interact with said at least one other computer entity.

3. The method as claimed in claim 1, wherein said process of managing at least one other computer entity comprises: adopting a policy towards said at least one other computer entity, said policy selected from a set of pre-determined policies for determining a relationship between said computer entity and said at least one other computer entity.

4. The method as claimed in claim 1, wherein managing at least one other computer entity in said network comprises a process selected from the set: placing said at least one other computer entity in quarantine; controlling access by said at least one computer entity to a communal resources stored on said computer entity;

comprises: determining at least one policy by which said computer entity will interact with said at least one other computer entity.

3. The method as claimed in claim 1, wherein said process of managing at least one other computer entity comprises: adopting a policy towards said at least one other computer entity, said policy selected from a set of pre-determined policies for determining a relationship between said computer entity and said at least one other computer entity.

4. The method as claimed in claim 1, wherein managing at least one other computer entity in said network comprises a process selected from the set: placing said at least one other computer entity in quarantine; controlling access by said at least one computer entity to a communal resources stored on said computer entity;

<p>or applying a charge for utilisation by said at least one other computer entity of a communal resource.</p> <p>5. A method of managing a network comprising a plurality of peer to peer computers, said method comprising; at each said computer entity; determining locally at said computer entity a local policy for management of at least one target computer entity comprising said network; receiving a plurality of local policy messages from a plurality of computer entities comprising said network, each said local policy message describing a local policy applied at a corresponding respective said computer entity to said target computer entity, and determining from said plurality of received local policy data, and from said locally generated local policy, a network management policy to be applied to said target computer entity by</p>	<p>or applying a charge for utilisation by said at least one other computer entity of a communal resource.</p> <p>5. A method of managing a network comprising a plurality of peer to peer computers, said method comprising; at each said computer entity; determining locally at said computer entity a local policy for management of at least one target computer entity comprising said network; receiving a plurality of local policy messages from a plurality of computer entities comprising said network, each said local policy message describing a local policy applied at a corresponding respective said computer entity to said target computer entity, and determining from said plurality of received local policy data, and from said locally generated local policy, a network management policy to be applied to said target computer entity by</p>
--	--

<p>said local computer entity.</p> <p>6. The method as claimed in claim 5, further comprising: broadcasting said network policy to a plurality of peer computers within said network.</p> <p>7. The method as claimed in claim 5, comprising: monitoring said at least one target computer entity; and depending upon a result of said monitoring, adopting a pre-determined policy from a stored set of policies, and applying said policy to said at least one target computer entity.</p> <p>8. The method as claimed in claim 5, wherein a said policy comprises a policy selected from the set: a policy for determining whether or not to place a faulty computer entity into quarantine; a policy for generating a virus alert message for alerting other computer entities in the network that a said target computer entity has a virus; a policy for generating a fault</p>	<p>said local computer entity.</p> <p>6. The method as claimed in claim 5, further comprising: broadcasting said network policy to a plurality of peer computers within said network.</p> <p>7. The method as claimed in claim 5, comprising: monitoring said at least one target computer entity; and depending upon a result of said monitoring, adopting a pre-determined policy from a stored set of policies, and applying said policy to said at least one target computer entity.</p> <p>8. The method as claimed in claim 5, wherein a said policy comprises a policy selected from the set: a policy for determining whether or not to place a faulty computer entity into quarantine; a policy for generating a virus alert message for alerting other computer entities in the network that a said target computer entity has a virus; a policy for generating a fault</p>
---	---

<p>alert message for alerting other computer entities in the network that said target computer entity is faulty; a policy determining whether to exclude said target computer entity from accessing a particular type of resource; a policy for determining whether to exclude said target computer entity from the network; a policy for control of access by said target computer entity to a communal resource; a charging policy for charging said target computer entity for accessing a resource.</p> <p>9. The method as claimed in claim 5, comprising applying a monitoring operation to said target computer entity, said monitoring operation selected from the set: a monitoring operation for remote virus scanning of said target computer; a monitoring operation for observing a group behavior of a group of target computer entities within said network; a monitoring</p>	<p>alert message for alerting other computer entities in the network that said target computer entity is faulty; a policy determining whether to exclude said target computer entity from accessing a particular type of resource; a policy for determining whether to exclude said target computer entity from the network; a policy for control of access by said target computer entity to a communal resource; a charging policy for charging said target computer entity for accessing a resource.</p> <p>9. The method as claimed in claim 5, comprising applying a monitoring operation to said target computer entity, said monitoring operation selected from the set: a monitoring operation for remote virus scanning of said target computer; a monitoring operation for observing a group behavior of a group of target computer entities within said network; a monitoring</p>
--	--

<p>operation for detecting a security breach in said network; a monitoring operation for detecting a performance problem of said at least one target computer.</p>	<p>operation for detecting a security breach in said network; a monitoring operation for detecting a performance problem of said at least one target computer.</p>
<p>10. The method as claimed in claim 5, wherein said step of determining a network management policy comprises: applying a voting protocol for adopting a common policy amongst a plurality of said computer entities.</p>	<p>10. The method as claimed in claim 5, wherein said step of determining a network management policy comprises: applying a voting protocol for adopting a common policy amongst a plurality of said computer entities.</p>
<p>11. A computer entity comprising: a peer to peer networking component for allowing said computer entity to engage other computer entities on a peer to peer basis; and a network management component for enabling a said computer entity to participate in management of a peer to peer network, wherein said network management component is configured to operate a process for managing at least one other said computer entity in said</p>	<p>11. A computer entity comprising: a peer to peer networking component for allowing said computer entity to engage other computer entities on a peer to peer basis; and a network management component for enabling a said computer entity to participate in management of a peer to peer network, wherein said network management component is configured to operate a process for managing at least one other said computer entity in said</p>

network, whenever said resources are not being used by at least one service application at a higher level layer than said peer to peer protocol.

12. The computer entity as claimed in claim 11, configured such that said management component is activated whenever said peer to peer network component is operational.

13. The computer entity as claimed in claim 11, wherein said network management component comprises a program data which controls said resources to perform a network management service.

14. The computer entity as claimed in claim 11, wherein said network management component operates to apply at least one policy for determining a mode of operation of said computer entity in relation to at least one other said computer

network, whenever said resources are not being used by at least one service application at a higher level layer than said peer to peer protocol.

12. The computer entity as claimed in claim 11, configured such that said management component is activated whenever said peer to peer network component is operational.

13. The computer entity as claimed in claim 11, wherein said network management component comprises a program data which controls said resources to perform a network management service.

14. The computer entity as claimed in claim 11, wherein said network management component operates to apply at least one policy for determining a mode of operation of said computer entity in relation to at least one other said computer

entity of said network. 15. The computer entity as claimed in claim 11, wherein said network management component operates to: communicate with a plurality of other computer entities of said network for sending and receiving policy data concerning an operational policy towards a target computer entity; and determine, from a consideration of policy data received from said other computer entities, a global policy to be adopted by each computer entity in said network, towards a said target computer entity. 16. A data storage media comprising program data for controlling a computer entity to participate in a peer to peer network, said program data comprising instructions for: operating a peer to peer protocol for enabling said computer entity to utilise resources of at least one other	entity of said network. 15. The computer entity as claimed in claim 11, wherein said network management component operates to: communicate with a plurality of other computer entities of said network for sending and receiving policy data concerning an operational policy towards a target computer entity; and determine, from a consideration of policy data received from said other computer entities, a global policy to be adopted by each computer entity in said network, towards a said target computer entity. 16. A data storage media comprising program data for controlling a computer entity to participate in a peer to peer network, said program data comprising instructions for: operating a peer to peer protocol for enabling said computer entity to utilise resources of at least one other
---	---

computer entity of said network, and for enabling at least one other said computer entity of said network to utilise resources of said computer entity; and operating a process for managing at least one other said computer entity in said network, whenever said resources are not being used by at least one service application at a higher level layer than said peer to peer protocol.	computer entity of said network, and for enabling at least one other said computer entity of said network to utilise resources of said computer entity; and operating a process for managing at least one other said computer entity in said network, whenever said resources are not being used by at least one service application at a higher level layer than said peer to peer protocol.
---	---

This is a provisional obviousness-type double patenting rejection.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3, 5-7 and 10 –20 are rejected under 35 U.S.C. 102(e) as being anticipated by Pabla et al. (US Patent 7,127,613, hereinafter Pabla).

Regarding claim 1, Pabla discloses *a method for controlling a computer entity to participate in a peer to peer network of a plurality of computer entities* (Fig. 6 and Col. 13, lines 6 –13), said method comprising:

for each computer entity (Fig. 1B, 104):

operating a peer to peer protocol for enabling said computer entity to utilize resources of at least one other said computer entity of said network, and for enabling at least one other said computer entity of said network to utilize resources of said computer entity (Col. 13, lines 17 –25 and Col. 19, lines 32 –40).

operating a process for managing at least one other said computer entity in said network, whenever said resources are not being used by at least one service application at a higher level layer than said peer to peer protocol (Fig. 13, Col. 20, lines 44 – Col. 21, lines 16).

Regarding claim 2, Pabla discloses *the process of managing at least one other computer entity in said network comprises: determining at least one policy by which said computer entity will interact with said at least one other computer entity* (Col. 13, lines 9 – 14 and lines 51 -66).

Regarding claim 3, Pabla discloses *the process of managing at least one other computer entity comprises* (Col. 13, lines 55 –58):

adopting a policy towards said at least one other computer entity, said policy selected from a set of pre-determined policies for determining a relationship between said computer entity and said at least one other computer entity (Col. 17, lines 44 - 63,.

Regarding claim 5, Pabla discloses *a method of managing a network comprising a plurality of peer to peer computers (Fig. 1B) said method comprising;*

at each said computer entity (Fig. 1B, 104);

determining locally at said computer entity a local policy for management of at least one target computer entity comprising said network (Col.19, lines 1- 5 and lines 38 – 40);

receiving a plurality of local policy messages from a plurality of computer entities comprising said network (Fig. 10, lines 29 –32), each said local policy message describing a local policy applied at a corresponding respective said computer entity to said target computer entity (Col. 17, lines 23- 40 and Col 18, lines 55 –59),

determining from said plurality of received local policy data, and from said locally generated local policy, a network management policy to be applied to said target computer entity by said local computer entity (Col. 21, lines 13- 16 and Col. 24, lines 15 –23).

Regarding claim 6, Pabla discloses *the method as claimed in claim 5, further comprising: broadcasting said network policy to a plurality of peer computers within said network (Col. 17, lines 23 –31 and Col. 20, lines 33 –35).*

Regarding claim 7, Pabla discloses *the method comprising:*
monitoring said at least one target computer entity (Fig. 9, Col. 13; lines 6 –13);
depending upon a result of said monitoring, adopting a pre-determined policy
from a stored set of policies, and applying said policy to said at least one target
computer entity (Col. 13, line s51 –57).

Regarding claim 10, Pabla discloses *the step of determining a network*
management policy comprises: applying a voting protocol for adopting a common policy
amongst a plurality of said computer entities (Col. 18, lines 17 –32).

Regarding claim 11, Pabla discloses *a computer entity (Fig. 1B, 104) comprising:*
a peer to peer networking component for allowing said computer entity to engage
other computer entities on a peer to peer basis (Col. 12, lines 36 –67, Col. 20, lines 33 –
43, Col. 25, lines 44 –52).

a network management component for enabling a said computer entity to
participate in management of a peer to peer network (Fig. 13, Col. 20, lines 58 –63)

the network management component is configured to operate a process for
managing at least one other said computer entity in said network, whenever said
resources are not being used by at least one service application at a higher level layer
than said peer to peer protocol (Fig. 13, Col. 21, lines 13- 16and Col. 19, lines 32 –39).

Regarding claim 12, Pabla discloses *the computer entity as claimed in claim 11, configured such that said management component is activated whenever said peer to peer network component is operational* (Col. 17, lines 54 –63, Col. 18, lines 60 –63 and Col. 23, lines 32 –39) .

Regarding claim 13, Pabla discloses *the network management component comprises a program data which controls said resources to perform a network management service* (Col. 12, lines 55 –67, Col. 14, lines 44 –57, Col. 17, lines 29 –31, lines 39 –44 and Col. 19, lines 32 –39).

Regarding claim 14, Pabla discloses *the network management component operates to apply at least one policy for determining a mode of operation of said computer entity in relation to at least one other said computer entity of said network* (Col. 13, lines 9 –12 and Col. 17, lines 29 –31).

Regarding claim 15, Pabla discloses *the computer entity (104), wherein the network management component (Fig. 1B) operates to:*

communicate with a plurality of other computer entities of said network for sending and receiving policy data concerning an operational policy towards a target computer entity (fig. 10, Col. 13, lines 51 –57 , Col. 15, lines 51 –57, Col. 16 lines 61 – 62 and Col. 17, lines 29 –34 , lines 54 –56)

determine, from a consideration of policy data received from said other computer entities, a global policy to be adopted by each computer entity in said network, towards a said target computer entity (Col. 13, lines 55 –57 and Col. 18, lines 26 –39).

Art Unit: 2616

Regarding claim 16, Pabla discloses *a data storage media comprising program data for controlling a computer entity to participate in a peer to peer network* (Col. 12, lines 36 –67, Col. 13, lines 6 –12 and Col. 14, lines 44 –51), *said program data comprising instructions* (Col. 34, lines 49 – 64)for:

operating a peer to peer protocol for enabling said computer entity to utilize resources of at least one other computer entity of said network, and for enabling at least one other said computer entity of said network to utilize resources of said computer entity (Col. 13, lines 17 –23, Col. 19, lines 32 – 39 and Col. 20, lines 33 –43)

operating a process for managing at least one other said computer entity in said network, whenever said resources are not being used by at least one service application at a higher level layer than said peer to peer protocol (Fig. 13, Col. 20, lines 44 – Col. 21, lines 16).

Regarding claim 17, Pabla discloses *a method for controlling a computer entity to participate in a peer to peer network of a plurality of computer entities* (Fig. 1b,10 and Col. 18, lines 27 –32), *said computer entity comprising:*

a set of computing resources (Col. 13, lines 22 –23),

at least one higher level service provided by at least one service application (Col. 20, lines 46 49),

said method comprising:

operating a peer to peer protocol for enabling said computer entity to utilize resources of at least one other said computer entity of said network, and for enabling at least one other said computer entity of said network to utilize resources of said computer entity (Col. 13, lines 17 –25 and Col. 19, lines 32 –40).

operating a process for managing at least one other said computer entity in said network, whenever said resources are not being used by at least one service application at a higher level layer than said peer to peer protocol (Fig. 13, Col. 20, lines 44 – Col. 21, lines 16).

Regarding claim 18, Pabla discloses *the computer entity automatically operates said process for managing at least one other computer entity, in response to receipt of a service request from at least one of said plurality of computer entities, not including said computer entity itself (Col. 1, lines 32 –34, Fig. 13, Col. 18, lines 17 –32, Col. 20, lines 44 – 63 and Col. 21, lines 13 –16).*

Regarding claim 19, Pabla discloses *a method for controlling a computer entity to participate in a peer to peer network of a plurality of computer entities (Fig. 6 and Col. 13, lines 6 –13), said method comprising:*

for each computer entity (Fig. 1B, 104)::

operating a peer to peer protocol for enabling said computer entity to utilize resources of at least one other said computer entity of said network, and for enabling at least one other said computer entity of said network to utilize resources of said computer entity (Col. 13, lines 17 –25 and Col. 19, lines 32 –40).

operating said process for managing at least one other computer entity, in response to receipt of a service request from at least one of said plurality of computer entities, not including said computer entity itself (Fig. 13, Col. 20, lines 44 – Col. 21, lines 16).

Regarding claim 20, Pabla discloses a computer entity (Fig. 1B, 104) comprising:

a peer to peer networking component for allowing said computer entity to engage other computer entities on a peer to peer basis (Col. 12, lines 36 –67, Col. 20, lines 33 – 43, Col. 25, lines 44 –52).

a network management component for enabling a said computer entity to participate in management of a peer to peer network (Fig. 13, Col. 20, lines 58 –63)

the network management component is configured to operate a process for managing at least one other said computer entity in said network in response to receipt of a service request from at least one of said plurality of computer entities, not including said computer entity itself (Fig. 13, Col. 21, lines 13- 16and Col. 19, lines 32 –39).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. Claims 4 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pabla as applied to claims 1 and 5 above in the view of Gleichauf (US Patent 7,137,145, hereinafter Gleichauf), and further in view of Golle et al. (Incentives for Sharing in Peer-to-Peer networks, 2001, Stanford University, hereinafter Golle).

Regarding claim 4, Pabla discloses *the method of managing at least one other computer entity in said network* (Fig. 13, Col. 18, lines 17 –32, Col. 20, lines 33- 63 and Col. 21, lines 13 –16) *comprises a process selected from the set:*

controlling access by said at least one computer entity to a communal resources stored on said computer entity (Col. 13, lines 9 –14, Col. 15, lines 42 –44, Col. 18, lines 55 –59 and Col. 19, lines 66 –Col. 20, lines 2).

Pabla fails to explicitly teach *:placing said at least one other computer entity in quarantine;*

applying a charge for utilization by said at least one other computer entity of a communal resource.

However, Gleichauf teaches *placing said at least one other computer entity in quarantine* (Col. 2, lines 5 –10 and Col. 3, lines 63 – Col. 4, lines 11);

Gleichauf fails to teach *applying a charge for utilization by said at least one other computer entity of a communal resource.*

However, Golle teaches *applying a charge for utilization by said at least one other computer entity of a communal resource* (Page 1, lines 25 –34, page 5, lines 36 – 28).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Golle into the teaching of Pabla in combination with Gleichauf for the purpose of preventing penetration of the network

Art Unit: 2616

by hackers undetected, and increasing the system's value to its users and so make it more competitive with other commercial P2P systems.

Regarding claim 8, Pabla discloses *said policy comprises a policy selected from the set (Col. 21, lines 57):*

a policy for control of access by said target computer entity to a communal resource; (Col. 13, lines 9 –14, Col. 15, lines 42 –44, Col. 18, lines 55 –59 and Col. 19, lines 66 –Col. 20, lines 2).

Pabla fails to teach:

a policy for determining whether or not to place a faulty computer entity into quarantine

a policy for generating a virus alert message for alerting other computer entities in the network that a said target computer entity has a virus;

a policy for generating a fault alert message for alerting other computer entities in the network that said target computer entity is faulty;

a policy determining whether to exclude said target computer entity from accessing a particular type of resource ;

a policy for determining whether to exclude said target computer entity from the network ;

a charging policy for charging said target computer entity for accessing a resource.

However, Gleichauf teaches;

a policy for determining whether or not to place a faulty computer entity into quarantine (Col. 2, lines 5 -10Col. 3, lines 63 – Col. 4, lines 11, and Col. 12, lines 44 – 59)

a policy for generating a virus alert message for alerting other computer entities in the network that a said target computer entity has a virus (Col. 2, lines 14 –36);

a policy for generating a fault alert message for alerting other computer entities in the network that said target computer entity is faulty (col. 2, lines 14 –36 and Col. 6, lines 57 –62);

a policy determining whether to exclude said target computer entity from accessing a particular type of resource (Col. 6, lines 57 –62 and Col. 13, lines 32 –35);

a policy for determining whether to exclude said target computer entity from the network (Col. 1, line 64 –Col. 2, lines 5,Col. 2, lines 25 –28, Col. 2, and Col. 3, lines 54 –57) ;

Gleichauf fails to teach *a charging policy for charging said target computer entity for accessing a resource.*

However, Golle teaches *a charging policy for charging said target computer entity for accessing a resource* (Page 1, lines 25 –34, page 5, lines 36 –28).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Golle into the teaching of Pabla in combination with Gleichauf for the purpose of preventing penetration of the network by hackers undetected, and increasing the system's value to it users and so make it more competitive with other commercial P2P systems.

8. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pabla, and in the view of Gleichauf.

Regarding claim 9, Pabla discloses *the method comprising applying a monitoring operation to said target computer entity* (Col. 13, lines 6 –12), *said monitoring operation selected from the set:*

a monitoring operation for observing a group behavior of a group of target computer entities within said network (Col. 12, lines 55-67 and Col. 17, lines 29 –37) ;

a monitoring operation for detecting a security breach in said network (Col. 13, lines 9 –14, Col. 19, lines 66 –Col. 20, lines 10, Col. 25 , lines 61 – Col. 16, lines 3); *a monitoring operation for detecting a performance problem of said at least one target computer* (Col. 18, lines 45 – 50 and Col. 22, lines 17 – 31).

Pabla fails to disclose *a monitoring operation for remote virus scanning of said target computer*.

Art Unit: 2616

However, Gleichauf teaches a *monitoring operation for remote virus scanning of said target computer* (Col. 3, lines 39 –48 and Col. 9, lines 25 -28).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method teaching by Gleichauf into the method teaching by Pabla for the purpose of preventing penetration of the network by hackers undetected (Col. 3, lines 45 –48).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dady Chery whose telephone number is 571-270-1207.

The examiner can normally be reached on Monday - Thursday 8 am - 4 pm ESt.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ricky Q. Ngo can be reached on 571-272-3139. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Dady Chery 07/20/2007


RICKY Q. NGO
SUPERVISORY PATENT EXAMINER